SentinelOne

5 Strategies To Defend Against The Growing Risk Of Ransomware

eBook

Table of Contents

Every Year the Disruptive Impact of Ransomware Increases

How can organizations manage this risk to business continuity?

What does business disruption look like?

Recent ransomware incidents have painted some striking pictures, from casino slot machines plastered with error messages, to thousands of packages stacking up undelivered, to a nationwide fuel shortage

When a ransomware incident disrupts operations, the clock starts ticking, as **every hour that employees can't be productive** diminishes the organization's cash reserves and intensifies potential harm to customers and stakeholders. The risks go beyond the cost of downtime and can encompass permanently lost data or assets, reputational damage, legal consequences, sensitive data made public, and even the monetary impact of paying the ransom itself.

24 days

was the average length of interruption after a ransomware attack in 2022.[1]

1.1 billion USD

was paid out by victims of ransomware attacks in 2023.[2]

Why are we still talking about this?

Ransomware has been a top concern for cybersecurity experts for decades, and despite billions of dollars in investment in cybersecurity, the dollar cost of attacks grows ever higher. This topic has gained prominence in the public discourse due to recent high-profile attacks making headlines and has increasingly been the focus of government and regulatory attention.

This eBook seeks to answer the question of why the ransomware problem has proved so intractable while also offering five strategies that organizations can employ to preserve business continuity, even in a heightened threat environment. These strategies go beyond traditional perimeter protection to provide your organization with multiple robust lines of defense.

[1] Length of impact after a ransomware attack U.S., Statista, 2022

[2] State of Ransomware Report, ActualTech Media, 2024

Why is Ransomware Still So Persistent?

The battle between organizations and ransomware actors can often be asymmetric, since it's usually easier and cheaper to penetrate an environment than to protect it. Furthermore, because ransomware remains profitable, the balance of incentives continues to motivate highly specialized, persistent gangs of career cybercriminals.

Sophisticated, dynamic, and opportunistic threat actors

The world of ransomware is a complex ecosystem with highly specialized actors all along the kill-chain—from selling credentials, to ransomware-as-a-service (RaaS), to the actual group carrying out the extortion. These organizations move within a complex economy and function in a similar way to traditional businesses, with everything from partnerships and revenue models to marketing and recruitment. This landscape is constantly evolving, with prominent groups and tactics changing each week. Attackers systematically test environments, often with automation, and then focus attention on the areas where they find opportunities, meaning the battle is fought on the most favorable terrain for the attacker and the point of greatest weakness for the victim.

Under-resourced cybersecurity teams

Cybersecurity is an investment in risk mitigation. Like any expense, it is subject to budget scrutiny as organizations aim to avoid non-essential spending. However, these decisions come with a degree of uncertainty. Not all risks are readily apparent or quantifiable, and it can be difficult to find the right balance and determine how much is enough. It's like paying for a car insurance policy: it hurts when the money goes out every month, but you'll wish you had coverage if there's an incident.

Recent trends in evolving threats

Increasingly effective RaaS tools

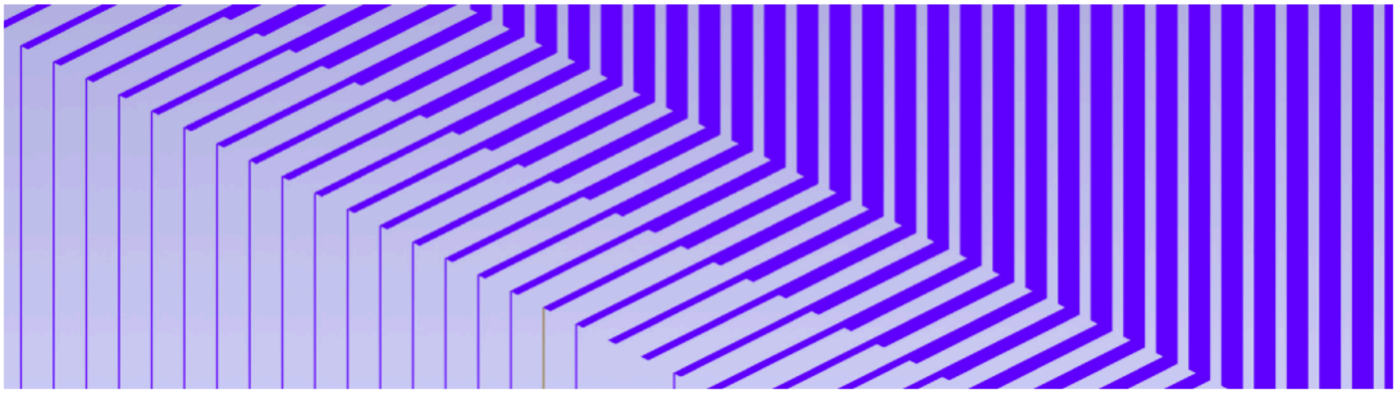
Ransomware-as-a-service is not a new phenomenon. However, the increasing sophistication of these inexpensive or free tools has lowered the barrier to entry for ransomware attacks while allowing kit developers to profit from extortion without assuming as much risk themselves. This has led to a splintering of the threat environment. With so many bad actors to track, it has become increasingly difficult to attribute attacks or distinguish the signal from the noise for targeted threat intelligence.

Remote monitoring and management exploitation

Cybercriminals are increasingly deploying remote monitoring and management (RMM) software as a persistent backdoor for command and control, and as a pipeline for data exfiltration. Bad actors will try a variety of RMMs to see what will bypass a particular firewall and use automated tools to create massive numbers of free trial accounts.

Compromised enterprise identity management

Attackers have taken advantage of exploits and zero-day vulnerabilities in multi-factor authentication (MFA) platforms to forge or intercept authentication tokens and bypass defenses.



The Challenges of Securing a Complex Environment

Humans are our greatest resource...

The community of cybersecurity professionals is one of extraordinary intelligence and creativity. However, growth of the of the workforce has struggled to keep pace with the explosion of new technology—leading to an endemic talent shortage and difficulty recruiting and retaining talent. In 2023, the gap between the demand for cybersecurity workers and the size of the actual workforce grew to almost four million.[1] Rapid digital transformation has created complex and fast-changing environments which are difficult to secure. Furthermore, most organizations use more than 40 cybersecurity tools, which creates complexity for security teams due to many interfaces and alert fatigue. Most teams are facing tough choices in terms of how they divide their time between activities like patching vulnerabilities, maintaining hygiene practices, meeting demanding compliance deadlines, threat hunting, and more. Under such circumstances, effective and systematic prioritization is paramount.

...and our greatest liability

Most successful ransomware attacks capitalize on human error rather than a purely technical vulnerability. An employee absentmindedly clicks what should be an obvious phishing email or simply visits the wrong website. This problem has become worse as attackers have increasingly taken advantage of new AI tools—such as generative AI programs that write convincing phishing emails at scale with far fewer grammatical errors or red flags. Under such circumstances, it's not prudent to assume that people will always make the right choices. Instead, organizations should assume a degree of human error and design accordingly.

Rapid innovation in the broader technology landscape has created environments that are more difficult to defend

Transition to the cloud

Cloud computing has profoundly changed the attack surface with new attack vectors such as cloud identities, APIs, and container security risks. It has also led to an explosion in the complexity of access control rules, further exacerbated by the increasing popularity of multi-cloud strategies.

Rise of work-from-home

Traditional network perimeters have been blurred in the cloud era, allowing attackers to bypass tools like firewalls. IT teams need to account for employees accessing resources from all over the world.

Proliferation of connected devices

The rise of the internet of things (IoT) has led to a dramatic increase in the number of connected devices, some of which may be agentless or historically air gapped. Furthearmore, many organizations permit their teams to access company resources on personal devices, which may also be unmanaged.

[1] Cybersecurity Workforce Study, ISC2, 2024

So, What is the Path Forward?

Given the relentlessness of threat actors and the resource constraints faced by organizations, what steps can be taken to reduce the risk of ransomware? In the following chapters, we'll cover five high-impact strategies to preserve business continuity, ranging from hardening your security posture, to detecting threats, to responding to incidents.

01 Illuminate Dark Corners of the Environment

02 Prevent "Patient Zero" with Identity Protection

03 Obstruct, Disrupt, and Misdirect Lateral Movement

04 Help Threat Hunters Look in the Right Places and Ask the Right Questions

05 Plan and Simulate a Worst-Case Scenario

01

Illuminate Dark Corners of the Environment

Attackers seek the path of least resistance

There are many ways to compromise an environment—from phishing, to brute force attacks, to entry through a corrupted website. The weakest points of the environment will often be the areas where IT lacks visibility. To fully understand an environment and its blind spots, it's important to take a holistic view that encompasses devices, identities, applications, the cloud, and more.

Many organizations face the challenge of "shadow IT," where employees or lines-of-business use devices, applications, or systems without the knowledge or support of the IT team. Sometimes these teams may simply be unaware of the security risk they are creating, or they may be seeking to avoid the perceived inconvenience of complying with security policies. The proliferation of connected devices and the rise of work from home have increased the number of unmanaged devices, which IT may not be aware of and therefore do not have agents installed. Legacy technology also poses a risk. Older hardware, applications, or websites may not be properly recorded on asset lists, or they may be incompatible with modern security protections.

Not only are all these resources not protected by IT, but if they are compromised, it will be much more difficult to detect suspicious activity. From the perspective of ransomware gangs, every unmanaged resource represents a possible entrance.

You can't protect resources you don't know about

Organizations should adopt a disciplined approach to maintaining an up-to-date asset list, with standardized processes and regular audits. Choosing the right tools can help them achieve an up-to-date list, since it helps teams discover devices and increase visibility over their environment. This is essential for preventing ransomware actors from gaining an initial foothold from which to find their way to your valuable data.

What do we mean by "dark corners"?

Unmanaged resources are not necessarily unusual or secret. Often, they are ordinary workstations or servers that have simply been overlooked. Here are some examples:

A software company acquires a startup. The complexity of the merger led some servers to be ignored in the compilation of a new centralized asset list.

A local government agency has a legacy website to help citizens navigate a now-defunct process. Role turnover and inadequate records have allowed this website to fall off the radar, and it is unmanaged and unprotected.

A healthcare company hires consultants to help them update their data estate. When the project is complete, the credentials established for the consultants are not offboarded.

Questions to ask when choosing an exposure management solution:

- **Can your solution discover cloud resources?**
- **Will this tool detect unmanaged identities?**
- **Does your solution look at your environment from the perspective of the attacker?**
- **Can your solution support both agent and agentless techniques?**

Combine discovery with vulnerability management

Both good and bad actors are constantly discovering new vulnerabilities, presenting organizations with a long and ever-changing list of weaknesses to tackle. Given the limited bandwidth of cybersecurity teams, prioritization is key.

Vulnerability management solutions can compare your asset list and installed applications against a list of known vulnerabilities and prioritize according to the degree of threat. However, this is only possible if the asset list is accurate and up to date, requiring network-wide visibility lest any “dark corners” or agentless devices be passed over. Bringing together vulnerability and exposure management allows organizations to discover unmanaged devices and unknown exposures. This in turn establishes a comprehensive view for identifying and prioritizing vulnerabilities.

Carefully assess your "bring-your-own-devices" policy

Although bring-your-own-devices (BYOD) policies may have benefits in terms of cost and convenience, unmanaged devices represent risks that must be managed. Consider the extent to which these devices can access sensitive data. Explore the possibility of making BYOD conditional on employees installing an agent on their device. A BYOD policy must be viewed holistically within the context of other defenses, such as multi-factor authentication (MFA) and password rotation to protect credentials.

The boundaries of the network have expanded and blurred, with the rise of hybrid cloud environments, the proliferation of connected devices, and the move towards remote work. This has created blind spots for security teams.

Investigate your inroads

It’s also important to consider which third-parties have access to your network, such as service providers, partner organizations, and IT providers. If an organization you work with is breached, it can impact your environment and business. In fact, supply chains cause an alarmingly high proportion of data breach incidents—62%, according to Verizon's annual report.1 Organizations should consider adopting regular assessments of third-party security postures, while also working to ensure that third-party access to the environment is limited to only the privileges that are necessary.

Consider asking your vendors and partners:

- What is your incident response plan?
- How soon will you notify me if you are breached?
- Are you using a standard framework to harden your security presence?
- When did you complete your most recent external audit, and what were the results?
- Do you perform regular penetration tests, vulnerability scans, or internal security audits?

What could third-party risk look like?

An organization engages with a third-party IT provider. This vendor puts an unprotected domain controller at the perimeter of the environment without the organization's knowledge. The security operations team has no visibility over this asset and cannot protect it or detect if it is compromised.

[1] Annual Data Breach Investigation Report, Verizon, 2022

02

Prevent "Patient Zero" with Identity Protection

Don't allow a compromised identity to grow into a full-scale attack

An adversary rarely, if ever, lands on the highest value machine at the start of an attack. Typically, an intruder will begin by targeting a weak point and then will seek access to other targets once inside an environment. Because of this, a threat actor's first step is often reconnaissance. The adversary will look for ways to move laterally through the network and elevate their privileges. They will seek to query the domain controller to discover who the domain admins are and then move to compromise those privileged identities. Attackers may use legitimate commands and pre-installed executables of the operating system to perform their actions. By leveraging these existing tools, attackers can avoid detection.

For business looking defend against this, the challenge is twofold:

1. How can you protect your identities from initial compromise?
2. How can you prevent a single compromised identity from becoming "patient zero" with malign influence spreading across the environment?

Considering the problem of social engineering

With sophisticated attacks, elaborate manipulation tactics, and generative AI-enhanced phishing messages, the battle against social engineering can feel hopeless. On one hand, security teams must always assume that some users will make mistakes that lead to compromised credentials and plan accordingly. That said, there are meaningful steps organizations can take to educate their teams. All employees should take a baseline level of social engineering awareness training that's reinforced by frequent, simulated phishing attempts. Role-based training can take this one step further by offering tailored training on the unique risks faced by specific roles, such as helpdesk staff or executives. Team members who handle sensitive information should be supported with robust policies and be aware of when and how to report suspicious requests.

29%

Of ransomware attacks involved compromised credentials asa root cause[1]

80%

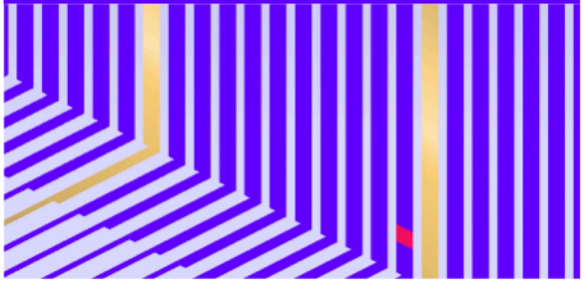
Of web application attacks used stolen credentials[2]

15 billion

Leaked credentials are circulating online, with a 143% increase in access broker dark web advertising in 2023[3]

40%

Of incidents involve phishing as the pathway to compromise making it the most common initial access vector[3]



[1] Root causes of ransomware attacks worldwide, Statista, 2023

[2] Tackling The Double Threat From Ransomware And Stolen Credentials, Forbes, 2022

[3] Cybersecurity Threat Trends Report, Deloitte, 2024

Security hygiene fundamentals checklist

- ✓ Use strong passwords with robust rotation and reuse policies
- ✓ Enable MFA (especially if permitting BYOD)
- ✓ Maintain accurate contact information for domain admins
- ✓ Avoid using domain admin credentials for everyday tasks
- ✓ Limit domain admin access to internet and vulnerable devices
- ✓ Keep the domain admin group small
- ✓ Use just-in-time access for privileged accounts

Avoid granting excessive privileges

- Implement role-based access controls and follow the principle of least privilege (PoLP)
- Conduct regular access reviews to confirm users still require their assigned privileges
- Leverage tools to automate workflows around provisioning deprovisioning and access requests
- Use separation of duties (SoD) to divide critical tasks across roles

If you haven't already... adopt universal MFA

Adopting multi-factor authentication (MFA) may seem like an obvious first step to securing your environment, but our incident response and forensics teams still see the lack of MFA as the common denominator in many breaches.

Most organizations that have not yet adopted MFA hesitate because of the friction imposed on the end-user. This security vs. convenience dilemma is common, and there is no universal answer to striking the right balance. That said, in the case of MFA, the security benefit in terms of risk reduction is huge. MFA adds an additional layer of protection to credentials against tactics such as brute force attacks or buying stolen credentials. Furthermore, MFA solutions can be configured to be minimally intrusive, while even increasing convenience in some cases by reducing the need for frequent password rotation.

Don’t forget to protect cloud identities

Cloud identities can serve as an easy target for bad actors (particularly for organizations without MFA) whether through a brute force attack or phishing. Today, cloud workloads are essentially an extension of the datacenter—which means that a compromised container can serve as launch point for an attacker to infiltrate the entire enterprise environment.

Detect compromised identities by looking for signs of unusual behavior

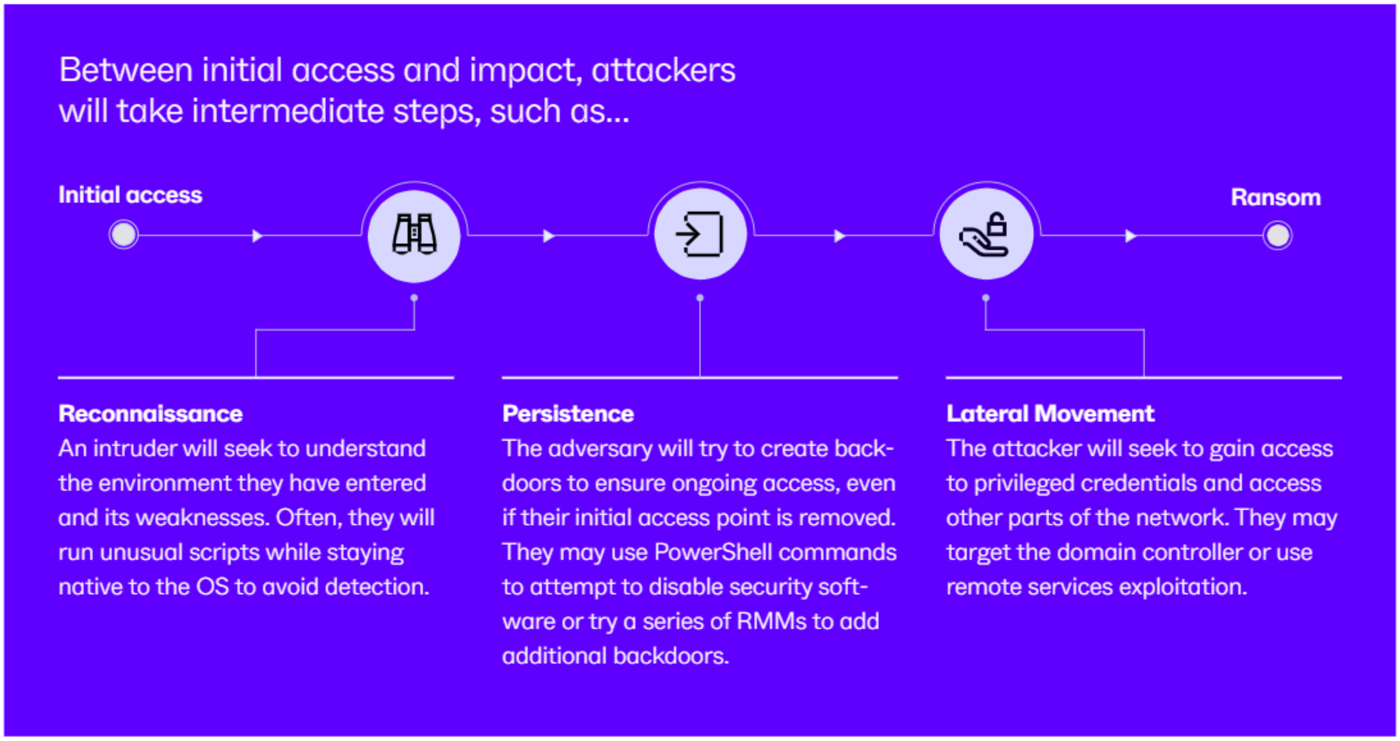
Often, there are telltale signs of a compromised identity. Think of it like this: normal users don't walk down a hallways and jiggle every doorknob. Examples of these indicators include hundreds of consecutive failed login attempts, consecutive login attempts from geographically distant locations, large quantities of exported data, and repeated domain controller queries. However, attackers are adept at avoiding detection, deploying tactics like impersonating trusted accounts or relying on OS native commands. Many organizations are using artificial intelligence to profile normal user behavior and detect deviations for review by the cybersecurity team. These tools can be combined with rule-based triggers which are configured and tailored to a particular user type or context, accounting for indicators flagged by threat intelligence.

03

Obstruct, Disrupt, and Misdirect Lateral Movement

Assume breach and design accordingly

In prior chapters, we explored ways to protect your resources and identities by establishing strong security hygiene practices. However, this alone is insufficient given the changing nature of the environment, with cloud computing and remote work blurring the boundaries of the network. Furthermore, organizations face sophisticated threats including credential theft, zero-day exploits and supply chain attacks. It's often not a question of if you will be breached, but when. Therefore, part of your strategy must entail planning for how you to manage intruders once they are inside your network. In the context of a ransomware attack, adversaries will opportunistically breach any device or identity that is vulnerable. Typically, the entry point differs from the final target—so in most cases, an attacker will need to move laterally or escalate privileges to get from an entry point to the proverbial "crown jewels."



Between initial access and impact, attackers will take intermediate steps, such as...

Reconnaissance
An intruder will seek to understand the environment they have entered and its weaknesses. Often, they will run unusual scripts while staying native to the OS to avoid detection.

Persistence
The adversary will try to create backdoors to ensure ongoing access, even if their initial access point is removed. They may use PowerShell commands to attempt to disable security software or try a series of RMMs to add additional backdoors.

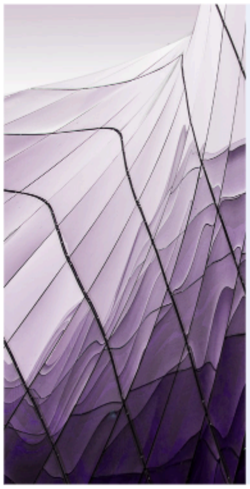
Lateral Movement
The attacker will seek to gain access to privileged credentials and access other parts of the network. They may target the domain controller or use remote services exploitation.

Don’t put all your eggs in one basket

Network segmentation is a method for obstructing lateral movement and preventing one compromised part from spreading to the whole. This is achieved by dividing a network into smaller, distinct subnetworks or segments. The most common method is through software-defined networking—in other words, defining rules and policies that determine which parts of the network can communicate. This means that sensitive areas can be isolated and clear dividing lines can be drawn between public-facing and internal resources. Organizations should create a heatmap of where sensitive data is located and maintain an up-to-date asset list (as discussed in the first chapter) to support effective segmentation design. Choosing the right tools can also support effective segmentation by reducing the complexity of configuring and maintaining policies.

Send adversaries on a wild goose chase

If a thief enters a castle, the last thing you would want is a map on the wall that tells them how to get to the vault. But what if you could offer them a fake map? Or lead them down a false staircase into a trap? Many organizations are employing deception technologies that do just this in the context of their network. This is possible by deploying realistic decoys alongside real assets including domains, databases, directories, servers, credentials and more. These decoys can be highly interactive to deceive attackers while providing valuable telemetry to support further investigation and attack intelligence for the security team. The result is that attackers end up wasting valuable time while taking actions that increase the probability of detection. This in turn makes the organization a less attractive target.



The importance of segmentation: A cautionary tale

A hospital utilizes a flat network architecture due to inherited legacy technology and budget constraints. This means that all assets within the hospital, including patient records systems, medical imaging devices, administrative computers, and even internet-connected medical devices, are all on the same network segment. A malicious actor compromises the network with stolen credentials belonging to a member of the admin staff. The lack of segmentation allows an adversary to move from a point of entry through the network, potentially compromising critical systems such as medical imaging archives, laboratory information systems, and even life-saving medical devices.

04

Help Threat Hunters Look in the Right Places and Ask the Right Questions

It’s as simple as asking, "what's this?"

In recent years, the timeline of a typical ransomware attack—from breach to encryption—has become significantly shorter. Mean time to detect and respond (MTTD and MTTR) are increasingly crucial metrics. For security operations teams, the key is to remain curious about your environment and actively look for suspicious behavior. Attacks can be prevented if the right person asks, “what’s this?” at the right time.

However, time is limited and it’s hard for analyst to be curious about an unusual signal if they have a long to-do list. Every organization faces the struggle to recruit and retain cybersecurity talent. Teams are stretched thin, and it’s difficult to make time for disciplined, systematic threat hunting. Furthermore, the barrier to entry is high. There are as many as 30 different syntax languages for threat hunting and none of them are intuitive. More broadly, many teams face the challenge of alert fatigue, where a constant stream of alerts makes it difficult to know what is truly urgent. In this chapter, we’ll explore three ways organizations can empower security operations teams and support effective prioritization.

Using dashboards to find the needle in the haystack

In a world with too many tasks and not enough time, prioritization becomes key. Informed prioritization requires visibility across the environment and quality threat intelligence. Often, security teams are siloed so that different data may be collected and managed by different groups—for example, cloud security and endpoint security might be handled by separate teams. Bringing information together from different sources is essential to gaining environment-wide visibility. However, in order for that data to be useable, it needs to be updated in real-time and put in a format so that it’s normalized and ready for analysis. A truly effective dashboard goes beyond aggregation and complements security operations workflows by providing the right information, to the right role, at the right time.

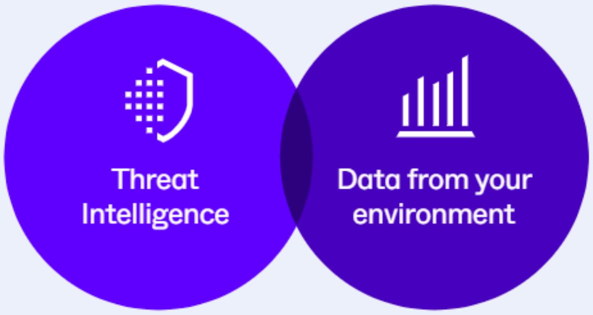
Questions to ask your vendor about dashboards:

- How does this tool go beyond information aggregation to provide coherence and prioritization?
- Is this tool designed and tested for specific security operations workflows?
- How does this dashboard meet the needs of different roles?
- Does this tool use a normalized data framework?
- Are the insights actionable?

Make better use of threat intelligence

Threat intelligence is crucial to helping organizations stay ahead of a dynamic threat landscape. The value of threat intelligence is not purely preventative. It can also enrich an investigation, adding context to an incident to accelerate mean time to detect and respond (MTTD and MTTR). This also poses dilemmas related to prioritization. Which threats are most urgent? Which vulnerabilities should you patch today, and which can wait? What information is most relevant to the incident you are investigating?

One place to look for answers is the meeting point of two datasets: threat intelligence and all the data you collect from your environment, such as telemetry, device lists, configuration data, and network traffic. AI can be used to analyze threat intelligence against your environment to determine which threats and vulnerabilities are most relevant to your environment and provide actionable next steps.

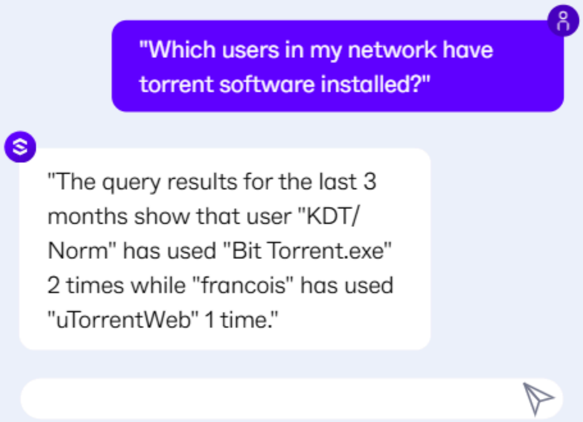


Combining threat intelligence with data from the environment can help security operations teams prioritize and contextualize threats within their organization's networks and systems.

Generative AI is a game-changer for threat hunting

Generative AI is a promising avenue to reduce the amount of time spent writing queries. These tools enable security professionals to interact with data through natural language which makes the task more accessible to less experienced analysts and helps more experienced analysts work faster and stretch their expertise further. In fact, it's a little like having an expert security analyst sitting beside you—someone who can answer your questions quickly and provide valuable insights in near real-time.

For example, an analyst can craft a query using natural language with generative AI assisting to write the code. Generative AI also supports detection and investigation by summarizing threat results in a conversational manner, so that the query outcome is easier to understand. These tools can suggest contextual follow-on queries, allowing analysts to dig deeper and stay ahead of attacks. AI can also reduce alert fatigue by offering guided recommendations to help teams prioritize which potential threats to prioritize and accelerate resolution by triggering automated workflows, like integration to the ticketing system.



"Which users in my network have torrent software installed?"

"The query results for the last 3 months show that user "KDT/Norm" has used "Bit Torrent.exe" 2 times while "francois" has used "uTorrentWeb" 1 time."

This is an example of a simple generative AI query and response. Often, the results will be more complex, such as a dataset with a bullet point summary.

05

Plan and Simulate a Worst-Case Scenario

No one wants to think about the worst thing that could happen

So why should you invest in incident response instead of simply concentrating your resources on prevention? The problem of securing a complex environment and preserving business continuity is fundamentally one of uncertainty. There are many variables, like human error and rapidly evolving threats, that cannot be fully known. The best way to mitigate risk in this context is through multiple robust lines of defense.

A ransomware attack is an extraordinarily stressful experience for the leaders of an organization, filled with long days and many difficult choices. A strong incident response playbook should **reduce the number of decisions that need to be made during a period of heightened stress and time pressure**.

Your plan should clearly specify the internal response team and third-party support with defined channels of communication. It should also lay out a policy for disclosing a breach to external stakeholders and a policy for whether payment of the ransom may be considered. Finally, an incident response plan includes recovery procedures. This consists of a depiction of what a worst-case scenario might look like, as well as measures to restore business continuity. Choosing the right recovery technology is also crucial, as every day of downtime is costly.

How prepared is your organization? Here are a few questions you should ask yourself to determine your readiness:

- How will you recognize and detect a ransomware breach?
- How will you contain the incident to prevent additional systems from being infected?
- How long would it take you to restore business continuity in the event of a ransomware attack?
- What is the cost per hour of downtime?
- Would you feel under pressure to pay?
- What steps can you take to reduce the leverage of a potential attacker?

Common incident response mistakes

Planning at the wrong level of detail

Writing a ransomware incident response plan that is not sufficiently detailed or that is too detailed to be usable.

Lack of secure communication channels

Using channels like IM apps or email can allow hackers to intercept and interfere with the communications of the incident response team.

Premature backup rebuilds

Initiating a rebuild without adequately diagnosing and remediating the original breach can mean that you're rebuilding from compromised systems, resulting in a second attack.

What steps can organizations take to improve their playbook?

Clearly define roles and responsibilities: Use job roles—not named individuals who may come or go—and define channels of communication and escalation paths.

Keep the war room small: A small, need-to-know group reduces risk of further compromise and confusion.

Know the experts you can lean on: Have appropriate third parties at the ready, with escalation paths that are understood by all stakeholders. These should include incident response, threat actor communications, insurance and legal counsel.

Practice the plan, for real: Conduct tabletop exercises to put your plan to the test and apply the learnings. These are typically hands-off-keyboards exercises. The goal is to ensure that all stakeholders understand the processes and the frameworks for making decisions in a crisis scenario.

The impact of poor planning: Indecision, delays and losses

Attackers gain access to a retail chain's network by exploiting vulnerabilities in their point-of-sale (POS) systems. Once inside the network, the attackers identify critical systems and deploy ransomware to encrypt data, disrupting store operations. The attackers demand payment for the decryption key. They threaten to leak sensitive customer information if the ransom is not paid promptly.

The IT team attempts to contain the incident, but valuable time is lost due to the lack of an effective escalation process. Leaders hesitate to disclose the breach and instead rumors spread, eroding trust in the brand. The retail chain hesitates to make critical decisions about whether to pay the ransom or attempt to recover the encrypted data, leading to further delays in restoration of operations.

Key learning: Lack of a clear plan on areas like escalation, disclosure and restoration lead to delayed, sub-optimal decisions in the context of a crisis.

Trends in ransom payments

29% Of ransomware victims paid ransoms in the fourth quarter of 2023.[1]

Of the victims that paid ransoms

41%

regained access after the first payment.[2]

59%

faced ongoing extortion for additional payments or never regained access to their data.[2]

Consider your backup technology

The traditional approach to backup is to take machines offline, wipe them (do a "truck roll"), and then perform a network restore. This method is time consuming, and during a ransom, the capacity for backup could be limited by the bandwidth of the network with too much data to move quickly.

Some organizations are investing in rollback remediation capabilities, which allow them to turn back the clock and restore machines to the last know good state. This is made possible by automatically capturing VSS snapshots at regular intervals and protecting them from alteration or compromise. This technology greatly reduces the risk to business continuity by allowing organizations to more quickly and reliably restore normal business operations.

Rollback remediation can reduce the time to restore from hours or days to mere minutes

[1] State of Ransomware Report, ActualTech Media, 2024

[2] Outcome for organizations after ransomware, Statista, 2023

Preserve Business Continuity and Safeguard Your Organization Against Ransomware

Cybersecurity professionals continue to grapple with a specialized, opportunistic and dynamic threats. The danger of ransomware threat remains a persistent and nebulous risk. It has become clear that preserving business continuity with confidence requires a multi-pronged approach, with multiple robust layers of defense aimed at resisting attacks and mitigating damage.

Choosing the right partners is vital to winning this battle. SentinelOne has unique capabilities to help you fight back at every stage of the kill-chain. These include:

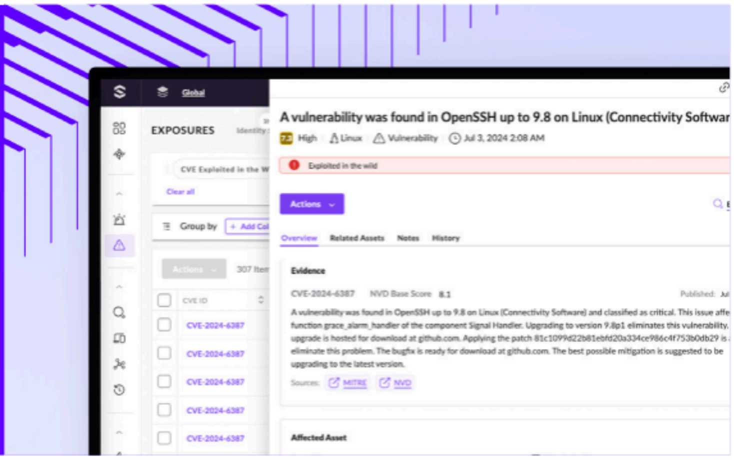
- Vulnerability and exposure management to help you illuminate dark corners
- Deception tools to obstruct, disrupt and misdirect
- Powerful generative AI capabilities, efficient dashboards and threat intelligence to support threat hunters
- Rollback remediation to help preserve business continuity in a worst-case scenario

Check out our website to learn more about the Singularity Platform or read our Purple AI Datasheet to learn more about how our generative AI capabilities can transform threat hunting.

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com



A vulnerability was found in OpenSSH up to 9.8 on Linux (Connectivity Softwar

Evidence

CVE-2024-6387 NVD Base Score 8.1 Published: Jul

A vulnerability was found in OpenSSH up to 9.8 on Linux (Connectivity Software) and classified as critical. This issue affe function grace_alarm_handler of the component Signal Handler. Upgrading to version 9.8p1 eliminates this vulnerability. upgrade is hosted for download at github.com. Applying the patch 81c1099d22b81ebfd20a334ce986c4f753b0db29 is eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP

TEVORA PCI DSS Attestation HIPAA Attestation

AICPA SOC

STAR LEVEL ONE

VB 100 VIRUS

SE Labs BEST Innovator WINNER 2021

Trusted Cloud Provider CSA

SentinelOne

Contact us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

eBook - SentinelOne Ransomware Thought Leadership 2024 08 27_08282024